Univerzita Karlova v Praze
Matematicko-fyzikální fakulta

ZÁZNAM O PRŮBĚHU OBHAJOBY DIPLOMOVÉ PRÁCE

Název práce: Algebraická teorie S-boxů

Jazyk práce: anglický

Jméno studenta/studentky: Bc. Elena Ďuránová

Studijní program: matematika

Studijní obor: matematické metody informační bezpečnosti

Vedoucí práce: Doc. RNDr. Jiří Tůma, DrSc.

Oponent/oponenti: Prof. RNDr. Aleš Drápal, DSc.

Členové komise:

Předseda:	**Prof. RNDr. Aleš Drápal, DSc. . - přítomen**
Místopředseda:	**Doc. RNDr. Jiří Tůma, DrSc. . - přítomen**
Členové:	**Mgr. Štěpán Holub, Ph.D. . - přítomen**
	RNDr. Přemysl Jedlička, Ph. D. . - přítomen
	RNDr. Petr Somberg, Ph. D. - přítomen
	Prof. RNDr. Ing. Petr Němec, DrSc. . - přítomen

Datum obhajoby: 28. 1. 2011

Průběh obhajoby: Diplomandka formou elektronické prezentace velmi zdařile zprostředkovala problematiku své práce. Poté přítomní vedoucí i oponent práce přečetli podstatné body ze svých posudků. Vedoucí práce zdůraznil přínos práce pro kryptografii a fakt, že je naděje na dosažení publikovatelného výsledku. Diplomandka odpověděla na výtky oponenta – vesměs šlo o potvrzení, že v práci se skutečně vyskytlo několik drobných nedopatření. V následné diskusi se vyjasnilo, že i když lineární nezávislost pro práci podstatných polynomů v předloženém textu dokázána není, diplomandka má takový důkaz k dispozici.

Výsledek obhajoby: ☑výborně ❑ velmi dobře ❑ dobře ❑ neprospěl/a

Předseda nebo místopředseda komise: Aleš Drápal

Pokyny pro předsedy nebo místopředsedy komisí:

Práce v elektronické podobě musí být studentem vložena do SIS. Formulář vyplňte ve všech bodech v elektronické podobě. V bodě Členové komise se uvedou všichni členové komise a za jejich jména se uvede „(přítomen)“ nebo „(nepřítomen)“. Předseda nebo místopředseda komise je jejím členem. V bodě Průběh obhajoby by měly být uvedeny alespoň čtyři věty vystihující průběh obhajoby. Po vyplnění formuláře ho vytiskněte, dole formulář ještě vlastnoručně podepište a přiložte k zápisu o státní závěrečné zkoušce. Současně vložte formulář v elektronické podobě (bez vlastnoručního podpisu) do SIS.